REMARKS/ARGUMENTS

The Applicant has amended claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set is fully supported by the originally filed specification.

Specifically the Examiner is referred to Fig. 4 and page 38, line 31 to page 42, line 28 for support.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 4-7 of the Office Action, the Examiner rejects claims 1, 3-5, 7-11 and 13-15 under 35 USC 102(e) as being anticipated by Shin *et al.* (US 5,987,134).

Amended claim 1 includes the limitation of "applying, in the trusted authentication chip, an asymmetric encryption function to the random number using a first key from the trusted authentication chip to produce an encrypted random number". Referring to col. 9, line 35 to col. 10, line 35, as cited by the Examiner, Shin *et al.* discloses only passing the random number integer r, having the value of C, being generated in the verification device 10, to the proving device 11. Nowhere does Shin *et al.* disclose encrypting the random number prior to "passing the encrypted random number to an untrusted authentication chip" as required in currently amended claim 1.

In Shin *et al.*, the proving device 11 then performs certain calculations based on the value of C. It is important to note that the user is required to supply identifying information e to be used in equation 6 (see col. 9, line 67 to col. 10, line 5). The presently claimed invention does not require user identifying information so that the untrusted authentication chip can be authenticated.

Furthermore, as an encrypted random number is not passed to the proving device of Shin *et al.*, the proving device 11 cannot perform the step of "decrypting, in the untrusted authentication chip, the encrypted random number with an asymmetric decryption function using a second secret key from the untrusted authentication chip to produce a decrypted random number" as is required in presently amended claim 1. Although modulo operations are performed on C this is not decryption of the encrypted random number passed to the proving device 11. Hence, the steps of currently amended claim 1 are not taken in Shin *et al.*

A further critical difference is that current claim 1 requires "comparing the decrypted random number with the original random number, without knowledge of the second secret key". It is explicitly stated, at col. 9, line 41 and col. 10, line 18 of Shin *et al.*, that both the exponent E and the modulus n are stored in the access ticket public key storing means 101. In the presently claimed invention the first key from the trusted authentication chip may be public, however, the "second secret key from the untrusted authentication chip" is required to be secret. This is an important difference which further highlights the differences between the present invention as claimed in independent claims 1 and 7 when compared to the disclosure of Shin *et al.* As the Examiner would be aware, in an asymmetric encryption method or system it is not a trivial matter to simply consider a public key and a secret private key as interchangeable.

The amendments to claim 1 are also reflected in currently amended claim 7, aforem ntioned arguments equally apply to currently amended syst m claim 7.

For at least the aforementioned reasons, it is respectfully submitted that independent claims 1 and 7 of the present application are not anticipated by or obvious in light of Shin *et al*, likewise, the dependent claims of the present application are respectfully submitted to be patentable over Shin *et al.*, and avoid the Examiner's 35 USC §103 rejection against claims 2, 6, 12 and 16, when taken individually or in combination with any of the prior art of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(e) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant: SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762